UNIVERSIDAD POLITÉCNICA SALESIANA
SEDE QUITO

CARRERA:
INGENIERÍA DE SISTEMAS

Trabajo de titulación previo a la obtención del título de:
Ingenieros de Sistemas

TEMA:
EVALUACIÓN DE TRES ATAQUES RANSOMWARE UTILIZANDO ESCENARIOS VIRTUALES COMO PLATAFORMA EXPERIMENTAL

AUTORES:
DANIEL ALEJANDRO AGUILAR NOBLECILLA
FRANKLIN RICARDO GUAITA VALLEJO

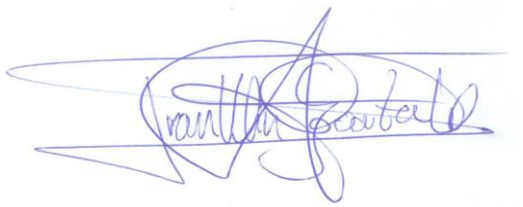
TUTOR:
FERNANDO JACINTO RODAS ORELLANA

Quito, agosto del 2018

CESIÓN DE DERECHOS DE AUTOR

Nosotros, Franklin Ricardo Guaita Vallejo con documento de identificación N° 1724406499, y Daniel Alejandro Aguilar Noblecilla con documento de identificación N° 1725600850, manifestamos nuestra voluntad y cedemos a la Universidad Politécnica Salesiana la titularidad sobre los derechos patrimoniales en virtud de que somos autores del trabajo de titulación con el tema: "EVALUACIÓN DE TRES ATAQUES RANSOMWARE UTILIZANDO ESCENARIOS VIRTUALES COMO PLATAFORMA EXPERIMENTAL", mismo que ha sido desarrollado para optar por el título de INGENIEROS DE SISTEMAS en la Universidad Politécnica Salesiana, quedando la Universidad facultada para ejercer plenamente los derechos cedidos anteriormente.

En aplicación a lo determinado por la Ley de Propiedad Intelectual, en nuestra condición de autores nos reservamos los derechos morales de la obra antes citada. En concordancia, suscribimos este documento en el momento que hacemos entrega del trabajo final en formato impreso y digital a la Biblioteca de la Universidad Politécnica Salesiana.



…….…...

DANIEL ALEJANDRO AGUILAR NOBLECILLA

CI: 1725600850

……...…….

FRANKLIN RICARDO GUAITA VALLEJO

CI: 1724406499

Quito, agosto del 2018

DECLARATORIA DE COAUTORÍA DEL TUTOR

Yo declaro que bajo mi dirección y asesoría fue desarrollado el Artículo académico, con el tema: "EVALUACIÓN DE TRES ATAQUES RANSOMWARE UTILIZANDO ESCENARIOS VIRTUALES COMO PLATAFORMA EXPERIMENTAL", realizado por Franklin Ricardo Guaita Vallejo y Daniel Alejandro Aguilar Noblecilla, obteniendo un producto que cumple con todos los requisitos estipulados por la Universidad Politécnica Salesiana, para ser considerados como trabajo final de titulación.

Quito, agosto del 2018

……

FERNANDO JACINTO RODAS ORELLANA

CI: 1708514821

Evaluación de tres ataques Ransomware utilizando escenarios virtuales como plataforma experimental

Fernando Rodas[1], Franklin Guaita[2], Daniel Aguilar[3]

Resumen

El Ransomware es un tipo de software malicioso destinado a infectar uno o varios dispositivos dentro de una red, dando la capacidad a un ciberdelincuente de encriptar los archivos y negar el acceso del usuario a toda la información almacenada.
En el presente trabajo se realiza una evaluación de tres ataques Ransomware: WannaCry, Jigsaw, y Petya. Como plataforma de experimentación se empleó un entorno virtual de red, el cual permite identificar cómo actúan dichos ataques en la encriptación de información; para esto se diseñó una red híbrida con segmentación WAN, LAN y DMZ que permite propagar el malware encriptando la información de los endpoints. La herramienta de simulación empleada para el diseño de la red fue GNS3. Para evaluar los ataques propuestos se desarrolló un mecanismo de infección controlado, empleando muestras de Ransomware compartidas en la web con fines educacionales. Finalmente, se evaluó el consumo de memoria, CPU y ancho de banda durante el ataque, con el fin de determinar cuál estos tres genera mayor impacto.

Palabras clave:
Ataque de seguridad, Encriptación, Jigsaw, Petya, Ransomware, WannaCry.

Abstract

Ransomware is a type of malicious software intended to infect one or several devices within a network, giving the ability to a cybercriminal to encrypt the files and deny the user access to all the stored information. In the present work an evaluation is made of three Ransomware attacks: WannaCry, Jigsaw, and Petya. As an experimentation platform, a virtual network environment was used, which allows to identify how said attacks act in the encryption of information; for this, a hybrid network with WAN, LAN and DMZ segmentation was designed to propagate the malware by encrypting the information of the endpoints. The simulation tool used to design the network was GNS3. To evaluate the proposed attacks, a mechanism of controlled infection was developed, using samples of Ransomware shared on the web for educational purposes. Finally, the consumption of memory, CPU and bandwidth during the attack was evaluated, to determine which of these generates the greatest impact.

Keywords:
Security attack, Encryption, Jigsaw, Petya, Ransomware, WannaCry.

[1] Magister en Gestión de las Comunicaciones y tecnologías de la información, Ingeniero en Sistemas, Docente de la carrera de Ingeniería de Sistemas – Universidad Politécnica Salesiana, Sede Quito – Campus Sur. Autor para correspondencia: frodasr@est.ups.edu.ec
[2] Estudiante de ingeniería de Sistemas – Universidad Politécnica Salesiana, Sede Quito – Campus Sur. Autor para correspondencia: fguaita@est.ups.edu.ec
[3] Estudiante de ingeniería de Sistemas – Universidad Politécnica Salesiana, Sede Quito – Campus Sur. Autor para correspondencia: daguilarn@est.ups.edu.ec

I. INTRODUCCIÓN

La tendencia al robo de datos bancarios e información personal ha tenido un incremento significativo en los últimos años, debido al mayor acceso a internet y a espacios donde se encuentra gran cantidad de información vulnerable.

A las herramientas de software empleadas para robar información a través de conexiones de internet se las denomina crimeware. [1]. Este término engloba una amplia gama de software de tipo maligno o potencialmente maligno. Dentro de estas categorías encontramos, por ejemplo, al pharming, adware, spyware, spoofing, y Ransomware [2]. Este último ha ganado mayor notoriedad debido a su modo de operar, tal como su nombre lo indica (ransom=rescate), se trata de un malware especializado en cifrar los archivos de un equipo para pedir un rescate o pago lo que permite obtener la legibilidad de los datos previamente alterados. [3]

El modo de actuar de los programas maliciosos Ransomware se guía por un esquema establecido. La infección inicia cuando un usuario descarga un archivo de un correo electrónico de spam o hace click en un link de internet. Una vez que el antivirus del equipo en cuestión falla, el programa se conecta con el servidor atacante para recibir instrucción.[4]. Cuando se logra infectar un ordenador, este trata de extenderse al resto de equipos conectados, ejemplo, a través de la red de la empresa. [5]

Según información de la corporación Manage Engine [6], el ataque cibernético más grande fue registrado en 2017, donde se evidenció un ataque masivo a escala global provocado por un tipo de Ransomware llamado WannaCry que afectó a empresas de telecomunicaciones, hospitales y compañías de reparto [7]. Sin embargo, otros Ransomware más sofisticados conocidos como Petya y Jigsaw han vulnerado la seguridad de otras organizaciones europeas. En el caso de Petya se dirige a computadoras con sistemas operativos Windows que no están actualizados [6] a diferencia de WannaCry, los datos perdidos nunca se pueden recuperar. Por otro lado, Jigsaw otra variedad de Ransomware, es una infección seria que puede infiltrarse en el sistema e intentar forzar al usuario a pagar dinero, el inconveniente es que no hay garantías de que conseguirá una clave de desencriptación. [8]

En torno a este problema, se ha desarrollado diversos estudios que profundizan la historia, caracterización, detección y mitigación del software malicioso Ransomware y sus variantes. En un estudio hecho por Jorge Ruíz denominado Ransomware: análisis y contramedidas se desarrolla un estudio general del Ransomware desde su primera aparición en 1989 hasta su estado actual, se analiza su modo de actuación y se enfatiza en su impacto en la sociedad. [9]. En el trabajo propuesto por Martínez Holzen, *Neutralización del ransomware criptográfico mediante un sistema de almacenamiento sincrónico versionado* se aborda el problema de cifrado de datos de manera no autorizada, y se plantea un esquema de almacenamiento con tecnología de nube, combinando el respaldo sincrónico con el control de versiones, para recuperar los datos afectados en caso de un ataque por Ransomware [10]. En el caso de estudio *Recuperación de datos cifrados mediante control de versiones en nube, una alternativa contra el ransomware* de Medina, Melquizedec; Martínez, Holzen se

analiza otra opción de mitigación de ataques por cifrado, este artículo presenta un caso de estudio del Ransomware, apoyado en una muestra open source destinada al análisis de este tipo de software, además, se presenta una propuesta que emplea una arquitectura basada en Dropbox para tener una recuperación ágil de los datos ante una eventual infección. [11]. En el *Estudio del ransomware en dispositivos móviles Android* realizado por Colomé se desarrolló un sistema para gestionar y realizar copias de seguridad de dispositivos móviles. [12]

El tema de la ciberdelincuencia no solo se asocia a factores científico-tecnológicos. Existen otras ramas de estudio que han centrado su atención en esta amenaza, por ejemplo, se realiza un análisis financiero donde se mide el movimiento de los flujos de pago correspondientes a ataques WannaCry. [13] Dentro del ámbito legal, se desarrolla aspectos de preservación y análisis de la evidencia digital asociada a este delito, para su consideración por parte del personal judicial [14].

En el presente trabajo se realiza una evaluación de tres ataques Ransomware: WannaCry, Jigsaw, y Petya. Se empleó un entorno virtual de red, que permite identificar el modo de operación de dichos ataques en la encriptación de información. Como plataforma de experimentación se diseña una red híbrida con segmentación WAN, LAN y DMZ que permite propagar el malware, encriptando la información de los endpoints. GNS3 fue la herramienta de simulación de red que se empleó sobre el sistema operativo Windows. Para evaluar los tres tipos de ataques propuestos se usó un mecanismo de infección controlado a partir de un Ransomware de la web con fines educativos.

El aporte de la presente investigación es la evaluación del consumo de memoria, CPU y ancho de banda durante el ataque mediante un análisis comparativo con el fin de determinar cuál de los tres ataques genera mayor impacto.

La investigación ha sido organizada en cinco apartados: I) Introducción, II) Fundamentos teóricos, III) Escenario de experimentación, IV) Pruebas y resultados obtenidos y V) Análisis comparativo de los resultados. Finalmente se presenta las conclusiones y la discusión trabajos futuros.

II. MARCO TEÓRICO

A. Ransomware

El Ransomware es un tipo de software malicioso cuyo objetivo es forzar a los usuarios a pagar un rescate para recuperar el acceso a su información. El pago por el rescate generalmente se realiza mediante Bitcoin o tarjetas prepago [15], dificultando el rastreo de los atacantes. El modo de infección generalmente es por la descarga de archivos de procedencia desconocida. De acuerdo con su forma de operar se lo puede clasificar en tres tipos [16]:

1. De bloqueo: Impide el funcionamiento normal de un dispositivo, dificultando la interacción usuario-dispositivo.
2. De cifrado: Cifra los archivos de una amplia gama de extensiones, afectando información personal del usuario. Existe una variedad de malware que ha evolucionado, llegando incluso a cifrar discos duros.
3. De control: Es el tipo de infección más peligroso, ya que accede y toma el control de sistemas completos, pudiendo afectar incluso a empresas a nivel mundial.

B. WannaCry

Es un virus del tipo Ransomware que afecta Windows y se propaga mediante el puerto 445/TCP (usado para acceder remotamente a través de la red y permitir comunicación entre aplicaciones) [15]. WannaCry permite que atacantes remotos ejecuten código arbitrario aprovechando la vulnerabilidad CVE-2017-0145 [16] de Microsoft.

C. Petya

Es otro virus del tipo Ransomware pero más sofisticado que WannaCry, pese a que se basa en el mismo principio de propagación masiva dentro de redes locales. Petya usa la vulnerabilidad de Microsft EternalBlue [17] junto a lo que se conoce en ciberseguridad como movimientos laterales. Petya es conocido como la próxima generación de WannaCry, y a diferencia de este, es capaz de apagar el ordenador o, al cabo de un tiempo, puede producir un apagado completo del sistema operativo. [18]

D. Jigsaw

Es una variedad de Ransomware conocida desde marzo de 2016. Jigsaw escanea el sistema de la víctima y encripta los archivos añadiendo la extensión .fun denegando el acceso a los mismos. Este tipo de Ransomware es muy peligroso, ya que cada hora se van eliminando alguno de los ficheros cifrados, e incluso tras pagar, no existe garantías de que se consiga una clave de desencriptación [19].

E. Actualización de seguridad

Específicamente en Windows, estas actualizaciones son pequeños parches diseñados para identificar problemas relacionados a agujeros de seguridad que han sido descubiertos recientemente. Estas actualizaciones generalmente se instalan automáticamente a través de Windows Update.

F. Software de virtualización

Programa informático que se instala en el sistema operativo anfitrión, y sirve de contenedor de máquinas virtuales, permitiendo además compartir recursos de hardware (CPU, memoria, disco duro), conexión a internet, y periféricos de entrada/salida [20].

III. ESCENARIO DE EXPERIMENTACIÓN

A. Herramientas

Los activos utilizados para el experimento fueron:

1) *Equipo anfitrión*

Una computadora Dell con sistema operativo Windows 7, procesador Intel Core i7-4510U y memoria RAM de 4GB. Esta máquina anfitriona es la encargada de dar soporte a la máquina virtual.

2) *Software de virtualización*

VirtualBox de Oracle que posee características de libre distribución, portabilidad, multihuéspedes, multiplataforma, además permite montar imágenes ISO *[21]*.

3) *Herramienta de simulación*

Software GNS3 que permite emular una gran variedad de IOS Cisco y redes Ethernet, ATM y switches Frame Relay *[22]*.

4) *Software de infección*

Los Ransomware WannaCry, Petya y Jigsaw son distribuidos con código abierto para fines netamente educativos. Su forma de operar es offline puesto que se trata de un método demostrativo. Los Ransomware WannaCry, Petya y Jigsaw se descargaron en paquetes zip desde las páginas https: *[23]*, *[24]* y *[25]* respectivamente, dichos archivos ocupan 240 KB como máximo.

En el experimento, los tres tipos de ransomware proceden de diferentes maneras: WannaCry encripta la información de los equipos conectados a la red, Petya cifra la tabla de archivos maestro MFT de los discos duros conectados a la red, y Jigsaw encripta la información y posteriormente la elimina.

B. Diseño de la topología experimental

Para generar ataques de encriptación se creó una infraestructura de red híbrida similar a la utilizada por cualquier red empresarial, como se muestra en la Fig. 1. De esta manera la topología de prueba consta de tres secciones:

1. Red de área local privada implementada dentro de una organización,
2. Red WAN para conexión entre organizaciones con servicios externos y usuarios remotos.
3. Zona DMZ o red perimetral entre la red local y una red virtual.

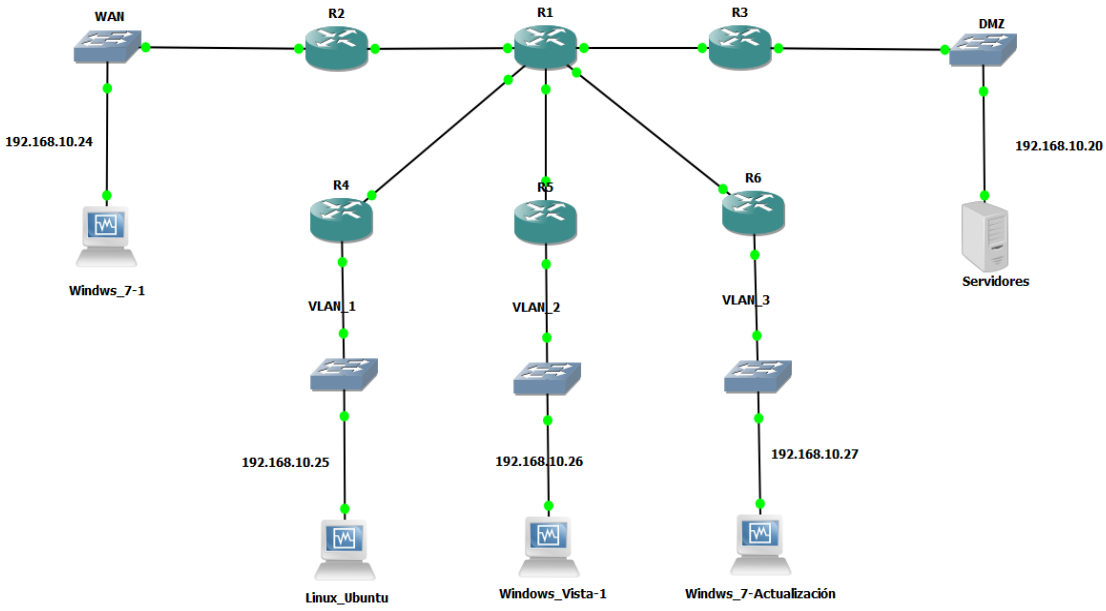


Fig. 1. Diseño para la generación de ataques Ransomware

C. Implementación de la plataforma experimental

Las pruebas se realizaron en diferentes máquinas virtuales con los siguientes sistemas operativos Windows Server 2012 r2, Windows 7, Windows vista, Linux Ubuntu respectivamente.

Como primer punto se empleó cinco enrutadores para la comunicación entre los dispositivos conectados a la red, en los cuales se configuro el protocolo de enrutamiento OSP. Como se muestra en la Tabla 1

Tabla 1
Tabla de enrutamiento

Dispositivo	Interfaz	Dirección IP	Mascar de subred
R1	S0/0	200.33.21.1	255.255.255.252
	S0/1	200.33.22.1	255.255.255.252
	S0/2	200.33.23.1	255.255.255.252
	S0/3	200.33.24.1	255.255.255.252
R2	S0/0	200.33.21.2	255.255.255.252
R3	S0/1	200.33.23.2	255.255.255.252
R4	S0/3	200.33.24.2	255.255.255.252
Servidor	NIC	192.168.10.20	255.255.255.0
PC 1	NIC	DHCP	255.255.255.0
PC 2	NIC	DHCP	255.255.255.0
PC 3	NIC	DHCP	255.255.255.0

A continuación, se crean cinco máquinas virtuales donde se realizaron las pruebas de infección de los tres tipos de ataques, cuyas características son:

4. Máquina virtual con Sistema Operativo Linux Ubuntu 16.04, procesador Core i5, memoria 1024 MB y almacenamiento 10 GB.
5. Máquina virtual con Sistema Operativo Windows vista de 32 bits, procesador Core i5, memoria 1024 MB y almacenamiento 20 GB.
6. Máquina virtual con Sistema Operativo Windows 7 de 32 bits, procesador Core i5, memoria 1024 MB y almacenamiento 20 GB, en la cual se instaló la actualización KB4012215 para evitar la propagación de ataque Ransomware dentro de la red híbrida.
7. Máquina virtual con Sistema Operativo Windows Server 2012 r2, procesador Core i5, memoria 1024 MB y almacenamiento 20 GB, en la cual se configuró el dominio DNS, los servicios FTP para la transferencia de archivos y DHCP para la distribución de direcciones IP, como se muestra en la Fig. 2.

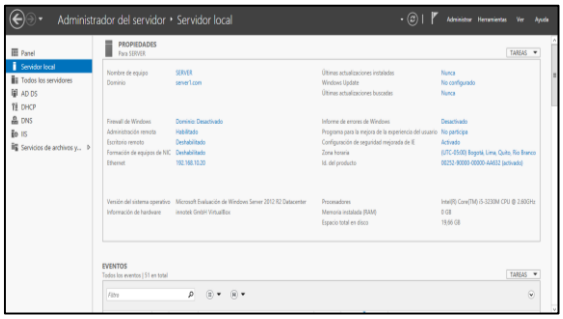


Fig. 2. Creación de servicios y dominio

D. Estructuración de servicios: DOMINIO, DHCP, FTP

Para la creación del servidor se empleó una IP estática 192.168.10.20/24 cuyo nombre de dominio es server1.com, como se muestra en la Fig. 3.

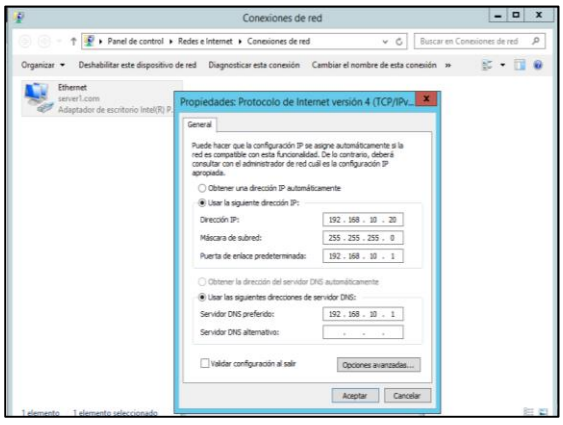


Fig. 3. Configuración del dominio del servidor

Posteriormente, se definió el rango de direcciones IP del servidor DHCP desde

192.68.10.21 hasta 192.168.10.40, como se muestra en la Fig.4, esto sirvió para la distribución automática de IP´S dentro de la red híbrida.

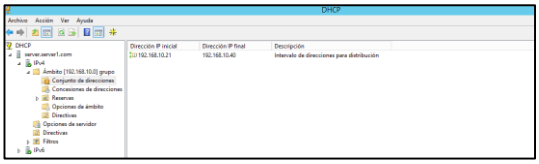


Fig. 4. Creación del servicio DHCP

Para transferir datos dentro de la red se configuró el servicio FTP en el servidor, se crea una carpeta que contiene los archivos a ser compartidos y de esta forma tener acceso desde cualquier navegador al ingresar a la dirección ftp: //192.168.10.20, como se muestra en la Fig.5.

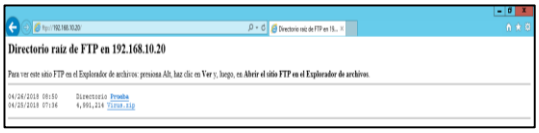


Fig. 5. Generación del servicio FTP

Para la ejecución del servicio FTP fue necesario la instalación previamente del servicio web IIS que facilita la publicación de información en Internet, permitiendo una autenticación robusta y segura para los usuarios. [26]

E. Generación de ataques

La generación de ataques Ransomware se realizó mediante la creación de un directorio activo también denominado Active Directory, en el cual se creó usuarios para conectar las distintas máquinas virtuales a nuestra red híbrida, como se muestra en la Fig. 6.

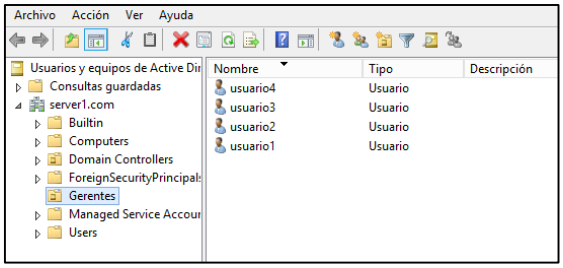


Fig. 6. Creación de usuarios

Una vez que las máquinas virtuales inician cesión con los distintos usuarios, el servidor se encarga de registrar las máquinas virtuales conectadas a la red, como se muestra en la Fig. 7

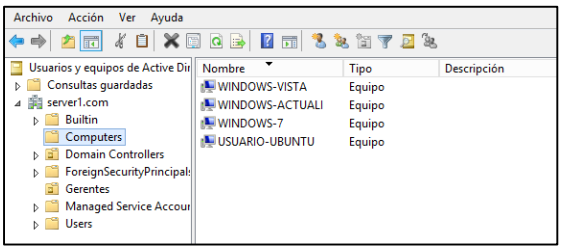


Fig. 7. Máquinas virtuales conectadas al servidor

Al generarse un ataque Ransomware en la red, pasa un tiempo para que se propague hacia todas las máquinas virtuales. Estos ataques se caracterizan por la propagación dentro de la red que compromete a las distintas máquinas virtuales conectadas al servidor, de esta forma secuestran la información y el equipo se vuelve obsoleto. Este ataque Ransomware se lo evidenció comparando el tiempo de propagación dentro de la red hibrida en los tres tipos de ataques.

IV. PRUEBAS Y RESULTADOS OBTENIDOS

*A. **Porcentaje de consumo de recursos al momento de activarse el ataque***

Para este análisis se realizó pruebas para cada tipo de ataque, y se calculó el porcentaje promedio de las mediciones del rendimiento de los recursos del equipo (consumo de CPU, memoria y ancho de banda) al momento de activar el ataque. Como se muestra en la Tabla 2.

Tabla 2
Consumo de recursos

Ataque / Porcentaje	Jigsaw	WannaCry	Petya
CPU %	100	90	0
Memoria %	40	38	0
Ancho Banda %	9	8	0

El ataque de tipo Jigsaw genera un gran daño en los recursos del equipo, en el consumo de CPU, memoria y ancho de banda provocando la saturación del CPU e impidiendo que se procesen peticiones dentro del equipo. A diferencia, el ataque de tipo WannaCry secuestra toda la información del disco duro en un solo proceso y no progresivamente como lo hace Jisaw.

El ataque Petya a pesar de no consumir recurso del equipo, (Tabla 2) es el más peligroso porque no permite al usuario ingresar al equipo. Este tipo de ataque secuestra todo el disco duro de forma inmediata y motivo por el cual no consume recursos.

Los resultados obtenidos de estas pruebas experimentales se muestran de manera gráfica en la Fig. 8.

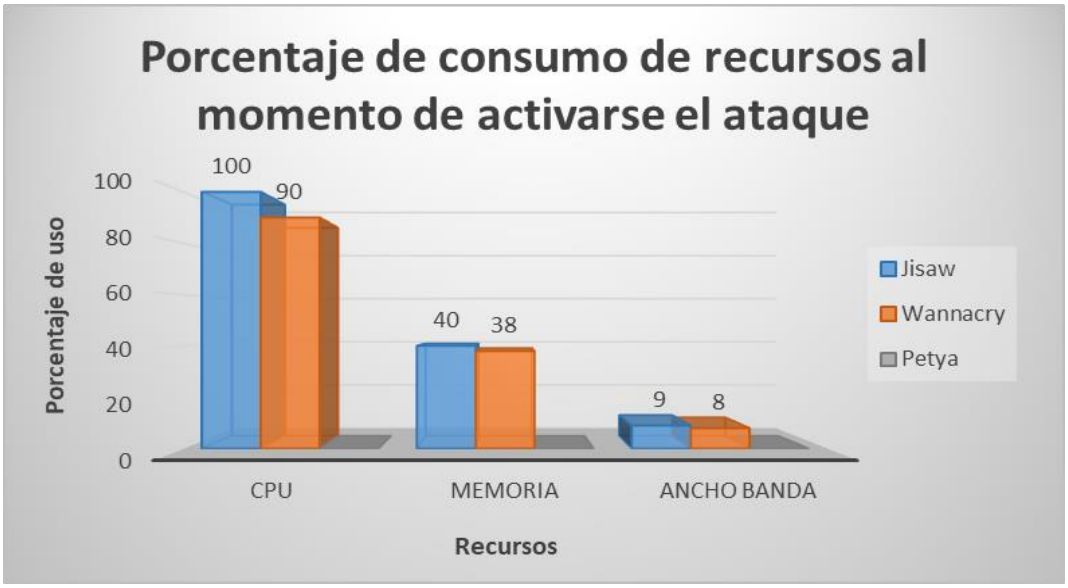


Fig. 8. Porcentaje de consume de recursos al momento de activar el ataque

B. Análisis de infección de los tres tipos de ataques en la red hibrida

Para el análisis de infección de los tres tipos de ataques se tomaron mediciones del rendimiento del sistema en las máquinas virtuales en tres casos diferentes: el punto de origen de la red LAN, el punto de origen de la red WAN, y en la red DMZ.

A continuación, para cada caso se realizaron 4 mediciones y se calculó el tiempo promedio de propagación del virus dentro de las redes LAN, WAN y DMZ.

C. Ataque Ransomware de tipo Petya

1) **Origen en la WAN:** Cuando el origen del ataque se generó en la WAN, el ataque inició en la máquina virtual Windows_7-1

tardo 60 minutos para infectarse, luego se propago a la LAN con la máquina Virtual Windows_Vista-1 en un tiempo de 35 minutos, y finalmente paso a la DMZ con la máquina virtual Servidores con un tiempo de 90 minutos.

2) **Origen en la LAN:** Cuando el origen del ataque se generó en la LAN, el ataque inició en la máquina virtual Windows_Vista-1 tardo 15 minutos para infectarse, luego se propago a la DMZ con la máquina virtual Servidores en un tiempo de 40 minutos, y finalmente paso a la WAN con la máquina virtual Windows_7-1 con un tiempo de 70 minutos.

3) **Origen en la DMZ:** Cuando el origen del ataque se generó en la DMZ, el ataque inició en la máquina virtual Servidores tardo 5 minutos para infectarse, luego se propago a la LAN con la máquina virtual Windows_Vista-1 en un tiempo de 35 minutos, y finalmente paso a la WAN con la máquina virtual Windows_7-1 con un tiempo de 90 minutos, como se observa en la Fig. 9.

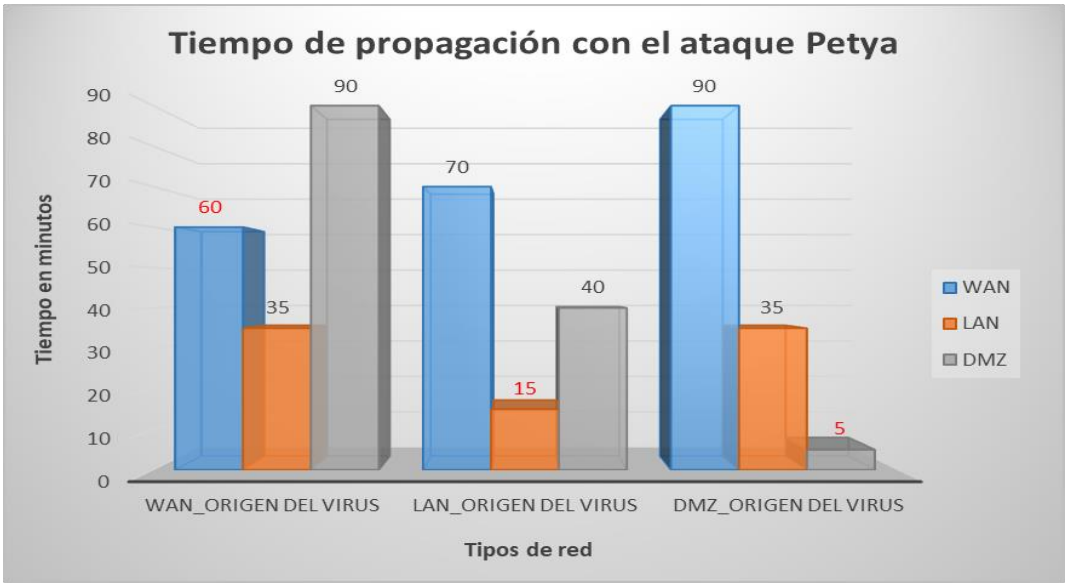


Fig. 9. Tiempo de propagación con el ataque Petya

D. Ataque Ransomware de tipo Jisaw

1) **Origen en la WAN:** Cuando el origen del ataque se generó en la WAN, el ataque inició en la máquina virtual Windows_7-1 tardo 70 minutos para infectarse, luego se propago a la LAN con la máquina Virtual Windows_Vista-1 en un tiempo de 45 minutos, y finalmente paso a la DMZ con la máquina virtual Servidores con un tiempo de 100 minutos.

2) **Origen en la LAN:** Cuando el origen del ataque se generó en la LAN, el ataque inició en la máquina virtual Windows_Vista-1 tardo 25 minutos para infectarse, luego se propago a la DMZ con la máquina virtual Servidores en un tiempo de 50 minutos, y finalmente paso a la WAN con la máquina virtual Windows_7-1 con un tiempo de 80 minutos.

3) **Origen en la DMZ:** Cuando el origen del ataque se generó en la DMZ, el ataque inició en la máquina virtual Servidores tardo 15 minutos para infectarse, luego se

propago a la LAN con la máquina virtual Windows_Vista-1 en un tiempo de 45 minutos, y finalmente paso a la WAN con la máquina virtual Windows_7-1 con un tiempo de 100 minutos, como se observa en la Fig. 10.

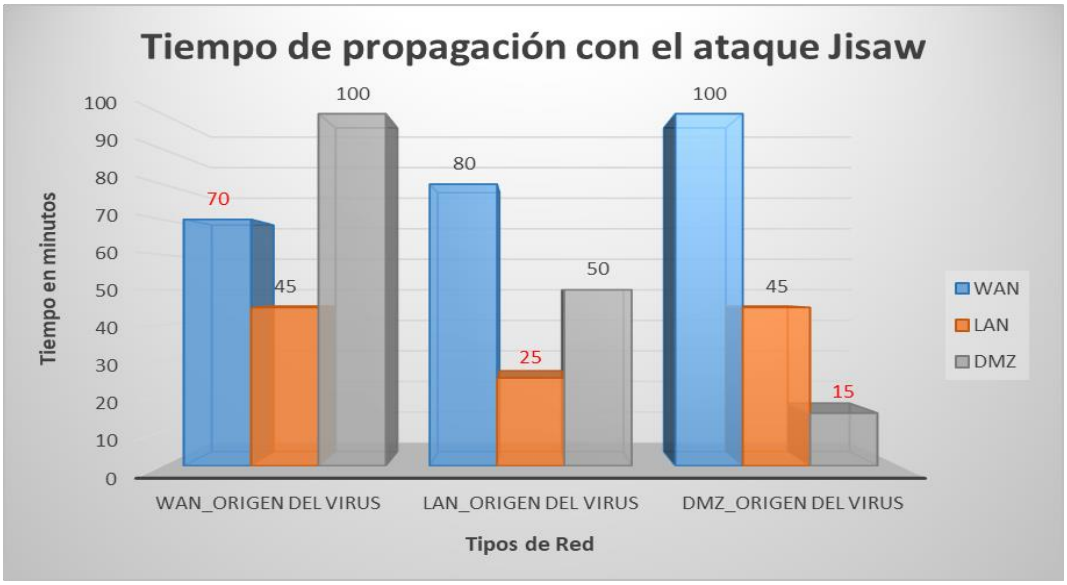


Fig. 10. Tiempo de propagación con el ataque Jisaw

E. ***Ataque Ransomware de tipo WannaCry***

1) **Origen en la WAN:** Cuando el origen del ataque se generó en la WAN, el ataque inició en la máquina virtual Windows_7-1 tardo 80 minutos para infectarse, luego se propago a la LAN con la máquina Virtual Windows_Vista-1 en un tiempo de 85 minutos, y finalmente paso a la DMZ con la máquina virtual Servidores con un tiempo de 110 minutos.

2) **Origen en la LAN:** Cuando el origen del ataque se generó en la LAN, el ataque inició en la máquina virtual Windows_Vista-1 tardo 35 minutos para infectarse, luego se propago a la DMZ con la máquina virtual Servidores en un tiempo de 60 minutos, y finalmente paso a la WAN con la máquina virtual Windows_7-1 con un tiempo de 90 minutos.

3) **Origen en la DMZ:** Cuando el origen del ataque se generó en la DMZ, el ataque inició en la máquina virtual Servidores tardo 25 minutos para infectarse, luego se propago a la LAN con la máquina virtual Windows_Vista-1 en un tiempo de 55 minutos, y finalmente paso a la WAN con la máquina virtual Windows_7-1 con un tiempo de 110 minutos, como se observa en la Fig. 11.

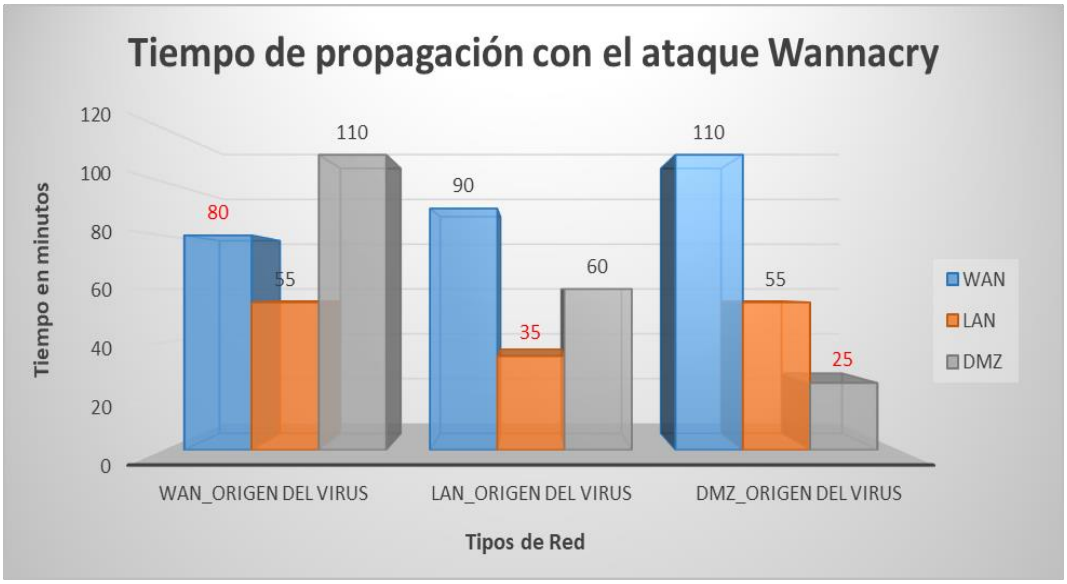


Fig. 11. Tiempo de propagación con el ataque WannaCry

F. ***Análisis comparativo de las tres tipas de redes***

Luego de analizar el comportamiento de los tres tipos de ataques dentro de la red fue necesario comparar el que genera mayor riesgo e impacto a la red de una organización:

1) Tiempo de propagación en la red WAN:

Se observó que al ejecutar los tres ataques Ransomware en la red WAN, el tiempo de propagación de los ataques Wannacry, Jigsaw, Petya tuvieron comportamiento diferente, como se muestra en la Fig. 12. Se describen en los siguientes casos:

a) Ransomware Wannacry. - En este ataque, el virus tuvo el mayor tiempo de propagación. Al inicio encripta toda la información de la máquina virtual Windows 7 tomando un tiempo estimado de 133 minutos. Posteriormente, el Ransomware Wannacry se propaga en las redes LAN y DMZ infectando las máquinas virtuales Windows_Vista-1 que se encuentra en la red LAN, tomando un tiempo estimado de 72 minutos. Por último, actúa sobre los Servidores que se encontraron en la red DMZ tomando un tiempo estimado de 72 minutos.

b) Ransomware Jigsaw. – Este ataque encripta la información de la máquina virtual Windows 7 con un tiempo estimado de 110 minutos. Posteriormente, el virus Ransomware Jigsaw infecta a las redes LAN y DMZ de las máquinas virtuales Windows_Vista-1 en un tiempo estimado de 69 minutos. Por último, actúa sobre los Servidores que se encuentra en la red DMZ en un tiempo estimado de 69 minutos.

c) Ransomware Petya. – Es el virus más peligro de entre los tres tipos de Ransomware. Al inicio toma un tiempo de 8 minutos para encriptar el disco duro. 90 minutos en reiniciar la máquina. Posteriormente, se transmite a las redes LAN y DMZ, infectando las máquinas virtuales Windows_Vista-1 en un tiempo de 63 minutos, finalmente, al Servidor, que se encuentra en la red DMZ, en un tiempo estimado de 62 minutos.

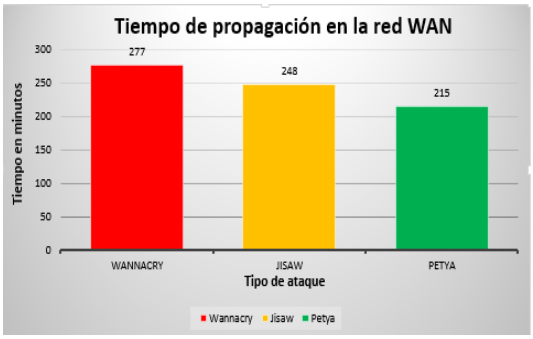


Fig. 12. Tiempo de propagación en la red WAN

2) Tiempo de propagación en la red LAN:

Al ejecutar los tres ataques en la red LAN, se tuvo tiempos variados en dichos ataques, como se muestra en la Fig. 13. Se observó un similar comportamiento de propagación en la red WAN. Se describe los siguientes casos:

a) Ransomware Wannacry. - Este ataque tuvo el mayor tiempo en expandir el virus. Al inicio, encripta toda la información de la máquina virtual Windows_Vista-1 en un tiempo de 110 minutos. Posteriormente, transmite el virus en las redes WAN y DMZ infectando las máquinas virtuales Windows 7 que se encuentra en la red WAN en un tiempo de 69 minutos. Por último, los Servidores que se encontraban en la red DMZ tomando un tiempo de 69 minutos.

b) Ransomware Jigsaw. - Este ataque, al inicio, encripta la información de la máquina virtual Windows_Vista-1 en un tiempo estimado de 5 minutos. Posteriormente, el virus se trasmite a las redes WAN y DMZ infectando las máquinas virtuales Windows 7 tomando un tiempo de 33 minutos. Por último, infecta a los Servidores que se encuentra en la red DMZ tomando un tiempo de 32 minutos.

c) Ransomware Petya. – Este ataque es el más peligroso. Toma un tiempo de 8 minutos para encriptar el disco duro, 4 minutos en reiniciar la máquina y transmitir el virus en las redes LAN y DMZ, infectando las máquinas virtuales Windows_Vista-1 en 24 minutos. Finalmente, el virus infecta a los Servidor, que se encuentra en la red DMZ, tomando un tiempo de 24 minutos.

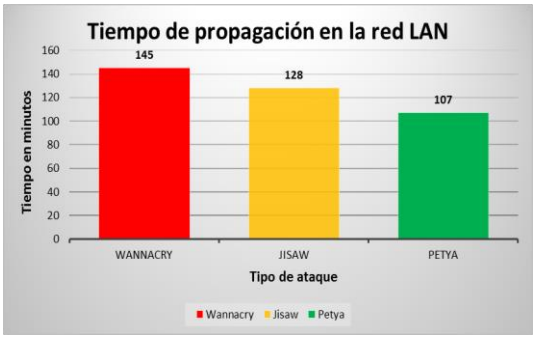


Fig. 13. Tiempo de propagación en la red LAN

3) Tiempo de propagación en la red DMZ:

Al ejecutar los tres ataques en la red LAN se observó un similar comportamiento de propagación de los Ransomware en la red WAN. Se tuvo tiempos variados en dichos ataques, como se muestra en la Fig. 14. Se describe los siguientes casos:

a) Ransomware Wannacry. - Este ataque tuvo el mayor tiempo de propagación en expandir el virus, el mismo que al inicio encripta toda la información de la máquina virtual Windows_Vista-1 en un tiempo de 10 min. Posteriormente, transmite el virus en las redes WAN y DMZ infectando las máquinas virtuales Windows 7, ubicado en la red WAN, tomando un tiempo de 35 min. Por último, el virus infecta a los Servidores, que se encontraba en la red DMZ, en un tiempo de 35 min.

b) Ransomware Jigsaw. – Este ataque, al inicio encripta la información de la máquina virtual Windows_Vista-1, tomado

un tiempo de 5 minutos. Posteriormente, trasmite el virus en las redes WAN y DMZ infectando las máquinas virtuales Windows 7, en un tiempo estimado de 33 minutos. Por último, el virus infecta a los Servidores que se encuentra en la red DMZ en un tiempo de 32 minutos.

c) Ransomware Petya. – Este virus es el más peligroso. En 8 minutos encripta el disco duro y 4 minutos en reinicia la máquina. Posteriormente, transmite el virus en las redes LAN y DMZ infectando las máquinas virtuales Windows_Vista-1, en un tiempo de 24 minutos. Finalmente, infecta a los Servidores, que se encuentra en la red DMZ, en un tiempo de 24 minutos.

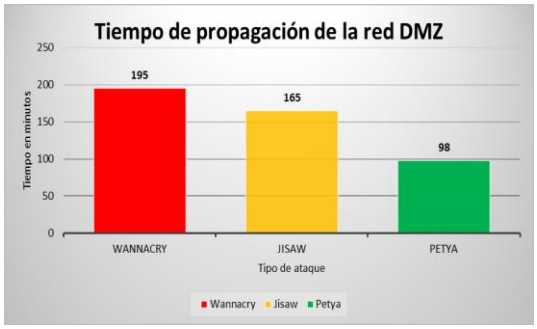


Fig. 14. Tiempo de propagación en la red DMZ

*G. **Periodo de tiempo para la liberación de archivos***

Para este análisis se realizó pruebas para cada tipo de ataque, se obtuvo el tiempo promedio en horas que tardan los tres ataques en secuestrar toda la información del disco duro. Como se muestra en la Tabla 3.

Tabla 3
Pérdida de archivos en horas

Ataques	Tiempo en horas
WannaCry	168
Jigsaw	72
Petya	1

El ataque WannaCry tarda 168 horas en infectar al equipo, los archivos se pierden y el equipo se vuelve obsoleto. Por otro lado, Jigsaw infecta al equipo y tarda 72 horas para que los archivos se pierdan en su totalidad. Finalmente, Petya es el que mayor impacto genera al infectar el equipo. Este tarda menos de una hora para que los archivos se pierdan en su totalidad. Como se muestra en la Fig. 15.

Fig. 15. Pérdida de todos los archivos

Es importante tomar en cuenta que para las máquinas virtuales Windows_7-Actualización y Linux_Ubuntu no se vieron afectadas por estos tres tipos de ataques, debido a que la máquina virtual Windows_7-Actualización no permite la propagación del ataque dentro de la red y solo infecta a equipos que no tengan actualizado su sistema operativos, en cuanto a la máquina virtual Linux_Ubuntu no permite la ejecución de estos ataques dentro de su sistema por ser un ataque que afecta a equipos con sistemas operativos Windows.

V. DISCUSIÓN

Como se observa en los resultados obtenidos en el capítulo anterior, el ataque por Ransomware ya sea de tipo Jigsaw, WannaCry o Petya genera alteraciones en los valores de los recursos del equipo en el

que se ejecuten, estos valores pueden o no ser significativos ya que la manera de atacar de los tres Ransomware es diferente. Por otro lado, el análisis del tiempo de propagación del virus dependiendo del punto de origen dentro de la red híbrida puede servir de guía a los administradores de red en el caso que deban tomar acciones frente a un ataque de este tipo.

Es importante mencionar que el estudio fue posible gracias a varios recursos: primero a la liberación de los Ransomware Jigsaw, WannaCry y Petya como open source presentados para efectos de estudio y análisis; segundo a las ventajas que ofrece la virtualización ya que permite evaluar diversos escenarios de experimentación sin la necesidad de emplear recursos físicos, dismuyendo costos, tiempo y riesgos de pérdida de información; por último al libre acceso de la herramienta de simulación que permite analizar el comportamiento del virus dentro de una red real.

Finalmente, una vez realizadas las pruebas respectivas de los tres tipos de Ransomware se aprecia que Jigsaw genera un mayor impacto negativo en los recursos del equipo, por un lado, provoca que se sature el CPU impidiendo que se procesen peticiones, genera un mayor uso de memoria y además un mayor consumo de ancho de banda ocasionando que el virus se propague con mayor rapidez dentro de la red, WannaCry genera un impacto menor que Jigsaw ya que este ransomware secuestra toda la información del disco en un solo proceso. Y Petya presenta valores de alteración nulos de los recursos del equipo ya que este Ransomware secuestra todo el disco de arranque del sistema operativo, y por tal razón no consume recursos.

VI. CONCLUSIONES

Ransomware es un tipo de virus o malware que impide o limita a los usuarios el acceso a sus recursos del sistema. Por lo tanto, en el presente trabajo está orientado al análisis y evaluación de tres ataques Ransomware en un ambiente virtualizado con el fin de perfeccionar técnicas de seguridad ante este tipo de ataques. Para implementar este trabajo se creó una topología de red virtual segmentando los accesos por la LAN, WAN y DMZ y obteniendo el ambiente virtual necesario para generar estos tipos ataques Ransomware. Se analizó las vulnerabilidades de los sistemas operativos Windows al no estar actualizados con sus últimas versiones.

Esta propuesta se pensó para prevenir tres tipos de Ransomware, que como ya se ha planteado, la tendencia hacia el robo de datos bancarios e información personal ha tenido un incremento significativo en los últimos años, sin embargo, se ha logrado analizar mecanismos de mitigación en los sistemas operativos de Windows. Sobre las máquinas virtuales infectadas se realizó el análisis de consumo de CPU, memoria y ancho de banda. Los resultados demuestran que los ataques consumen gran parte de los recursos al momento de la ejecución de los Ransomware.

Por último, los Ransomware: Jisaw, WannaCry, Petya son unos de los tipos de malware más peligroso actualmente, y una adecuada concientización de cómo actúa, así como tener el sistema operativo con las últimas actualizaciones siempre permite tomar medidas para minimizar el impacto de los ataques.

VII. REFERENCIAS

[1] F. Periáñez, "Características de VirtualBox: I.E.S. Mar de Cádiz," 2016. [Online]. Available: http://fpg.x10host.com/VirtualBox/caractersticas_de_virtualbox.html. [Accessed 22 Febrero 2018].

[2] B. Cristian, "Crimeware: el crimen del siglo XXI," 10 Septiembre 2009. [Online]. Available: https://www.welivesecurity.com/wp-content/uploads/2014/01/crimeware_crimen_siglo_xxi.pdf. [Accessed 19 Febrero 20018].

[3] Symantec, "Qué es el crimeware: Symantec.com," 2017. [Online]. Available: http://www.symantec.com/region/mx/avcenter/cybercrime/index_page3.html. [Accessed 1 Febrero 2018].

[4] Carbon Black, "Carbon Black Threat Report," 2017. [Online]. Available: https://www.carbonblack.com/wp-content/uploads/2016/12/16_1214_Carbon_Black-_Threat_Report_Non-Malware_Attacks_and_Ransomware_FINAL.pdf. [Accessed 16 Febrero 2018].

[5] P. Merino, "ecommercenews," 16 Mayo 2017. [Online]. Available: https://ecommerce-news.es/funciona-ataque-ransomware-infecto-telefonica-59957. [Accessed 16 Febrero 2018].

[6] Manage Engine, "Manage Engine," 2017. [Online]. Available: https://www.manageengine.com/products/desktop-central/secure-network-from-ransomware-and-cyber-attacks.html?gclid=EAIaIQobChMI27W57uCq2QIVD1mGCh0T4gtnEAAYASAAEgIBhfD_BwE. [Accessed 16 Febrero 2018].

[7] Symatec Official Blog, "WannaCry ransomware," 2017. [Online]. Available: https://www.symantec.com/blogs/threat-intelligence/wannacry-ransomware-attack. [Accessed 16 Febrero 2018].

[8] Avast, "Ransomware," 2017. [Online]. Available: https://www.avast.com/es-es/c-ransomware. [Accessed 16 Febrero 2018].

[9] A. Ruiz, "Ransomware,análisis y contramedidas:UAM_Biblioteca," Junio 2017. [Online]. Available: https://repositorio.uam.es/handle/10486/679544. [Accessed 19 Febrero 2018].

[10] H. Martínez, "Neutralización del ransomware criptográfico mediante un sistema de almacenamiento sincrónico versionado," 2017. [Online]. Available: https://www.grin.com/document/387405. [Accessed 19 Febrero 2018].

[11] M. Medina and H. Martínez, "Recuperación de datos cifrados mediante control de versiones en nube," Advances in Engineering and Innovation, vol. I, no. 1, p. 20, 2016.

[12] A. Colomé, "Estudio del ransomware en dispositivos móviles Android" Repositorio UAM. Mayo 2017. [Online]. Available: https://repositorio.uam.es/bitstream/handle/10486/679630/Soler_Colome_Alberto_tfg.pdf?sequence=1&isAllowed=y. [Accessed 19 Febrero 2018].

[13] V. Reyes and M. Salinas, "WannaCry: Análisis del movimiento de recursos," Research in Computing Science , p. 147, 2017.

[14] S. Trigo and C. Martín, "Ransomware: seguridad, investigación y tareas forenses," SID,

Simposio Argentino de Informática y Derecho, p. 130, 2016.

[15] F. Cesar, "Tercer Congreso Internacional de Ingeniería Informática," 2017. [Online]. Available: http://repositorio.pucp.edu.pe/index/bitstream/handle/123456789/71339/402%20Cesar%20Farro%20-%20Seguridad-Analisis%20de%20Ransomware%20(A204%2009.08.2017%2012.00).pdf?sequence=1. [Accessed 26 Marzo 2018].

[16] CERTSI, "Vulnerabilidad en SMBv1 en múltiples productos de Micorsoft Windows (CVE-2017-0145)," 15 Agosto 2017. [Online]. Available: https://www.certsi.es/alerta-temprana/vulnerabilidades/cve-2017-0145. [Accessed 26 Marzo 2018].

[17] Microsoft, "Microsoft Security Bulletin MS1-010-Critical," 2017. [Online]. Available: https://docs.microsoft.com/en-us/security-updates/securitybulletins/2017/ms17-010. [Accessed 22 Febrero 2018].

[18] ManageEngine, "Secure your network from Petya ransomware," 2017. [Online]. Available: https://www.manageengine.com/products/desktop-central/secure-your-network-from-petya-ransomware.html?cyber-attacks. [Accessed 22 Febrero 2018].

[19] G. Majauskas, "Jigsaw Ransomware: Malware," 2017. [Online]. Available: https://www.malwarerid.com/malwares/jigsaw-ransomware. [Accessed 22 Febrero 2018].

[20] A. González, "MAQUINAS VIRTUALES," 2015. [Online]. Available: https://iesvillalbahervastecnologia.files.wordpress.com/2016/02/maquinas-virtuales-dual.pdf. [Accessed 22 Febrero 2018].

[21] C. Balsa, "EMULACIÓN DE REDES CISCO CON GNS3: GNS3," 2016. [Online]. Available: http://www.adminso.es/recursos/Proyectos/PFM/2013_14/PFM_Aprende_GNS/Proyecto_Aprende_a_emular_redes_cisco_con_GNS3.pdf. [Accessed 22 Febrero 2018].

[22] J. De Nova, "TUTORIAL GNS3," 2015. [Online]. Available: https://jorgedenovasri.files.wordpress.com/2012/09/gns3.pdf. [Accessed 25 Mayo 2018].

[23] I. GitHub, "Ransomware.WannaCry_Plus," github.com, 10 05 2018. [Online]. Available: https://github.com/ytisf/theZoo/tree/master/malwares/Binaries/Ransomware.WannaCry_Plus. [Accessed 12 03 2018].

[24] I. GitHub, "Ransomware.Petya," github.com, 08 04 2016. [Online]. Available: https://github.com/ytisf/theZoo/tree/48220a4277c90d8eec5743e2a2b73a2eb1c7f97f/malwares/Binaries/Ransomware.Petya. [Accessed 05 03 2018].

[25] "Ransomware.Jigsaw," github.com, 13 04 2016. [Online]. Available: https://github.com/ytisf/theZoo/tree/8ffad0d46583dfd18ff3d87ea726424442838bc0/malwares/Binaries/Ransomware.Jigsaw. [Accessed 10 03 2018].

[26] M. d. e. d. España, "Definición de Servidor IIS," server.webcindario.com, 08 10 2003. [Online]. Available: http://2003server.webcindario.com/iis/definici.htm. [Accessed 18 02 2018].

[27] R. Lipovsky and L. Stefanco, "The Rise of Andrioid Ransomware," 2015, pp. 1-19.

[28] V. Reyes and M. Salinas, "WannaCry: Análisis del movimiento de recursos," Research in Computng Science, p. 149, 2017.

[29] J. Fernández, "WANNA CRY RANSOMWARE: Delitos tecnológicos CNP," 2017. [Online]. Available: JF Reyes - Quadernos de criminología: revista de criminología y …, 2017 - dialnet.unirioja.es. [Accessed 21 Febrero 2018].

[30] CNNESPANOL, "Qué es un virus 'ransomware' y cómo actúa: cnnespanol," 15 Mayo 2017. [Online]. Available: http://cnnespanol.cnn.com/2017/05/15/que-es-un-virus-ransomware-y-como-actua/. [Accessed 19 Febrero 2018].